ZEROFOX INTELLIGENCE

Flash

Threat Actor Claims Access to Identity Data

F-2026-09-03a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Data Breach, Threat Actor, Dark Web

September 3, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 10:00 AM (EDT) on September 3, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Actor Claims Access to Identity Data

| Key Findings

- On August 31, 2026, untested threat actor "databroker1" advertised a custom portal named "NEXUS" on the dark web forum Exploit, claiming the portal hosts a database of over 160 million breached identity documents.
- The actor claims to have maintained persistent access to an unnamed major identity verification provider and its enterprise clients (including several Fortune 500 companies) and conducted ongoing exfiltration for over a year, with approximately 500,000 new documents added daily.
- ZeroFox assesses that IDScan[.]net is very likely the vendor targeted by the threat actor; the company offers an identity verification platform in both digital and physical spaces. While IDScan[.]net has not made a public statement, several social media posts by customers claim that the company sent out an email about investigating a “potential security incident.”
- Although the NEXUS portal is no longer active, there is a roughly even chance the threat actor will reactivate access after a cooling-off period to let the public scrutiny die down. Additionally, the threat actor’s claim of persistence—as well as

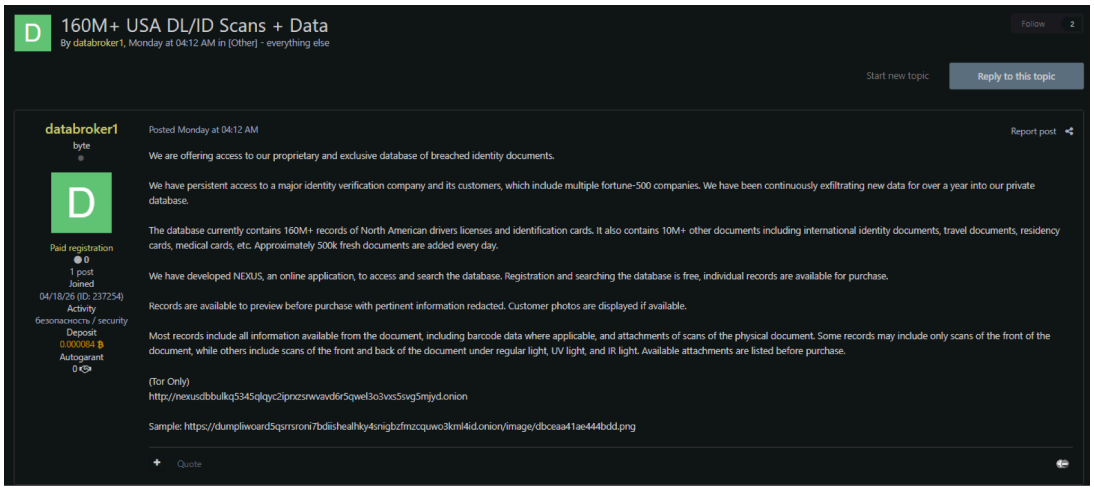
the extensive coverage of IDScan[.]net data potentially available—very likely makes this breach an ongoing threat to personal identity data.

Details

On August 31, 2026, untested threat actor databroker1 advertised a custom portal named NEXUS on the dark web forum Exploit, claiming the portal hosts a database of over 160 million breached identity documents. Contents of the NEXUS portal allegedly include:

- More than 150 million U.S. and Canadian driver's licenses
- At least 10 million identification cards
- Roughly three million travel documents and/or international IDs
- 579,000 medical cards[1]

The actor claimed to have maintained persistent access to an unnamed major identity verification provider and its enterprise clients (including several Fortune 500 companies) and conducted ongoing exfiltration for over a year, with approximately 500,000 new documents added daily. Furthermore, the actor stated that the NEXUS database is accessible via a Tor portal where users can register and search records at no cost while purchasing individual entries.



databroker1's original post on Exploit
Source: ZeroFox Intelligence

[1] hXXps://krebsonsecurity[.]com/2026/09/fbi-probes-service-selling-153m-drivers-licenses/

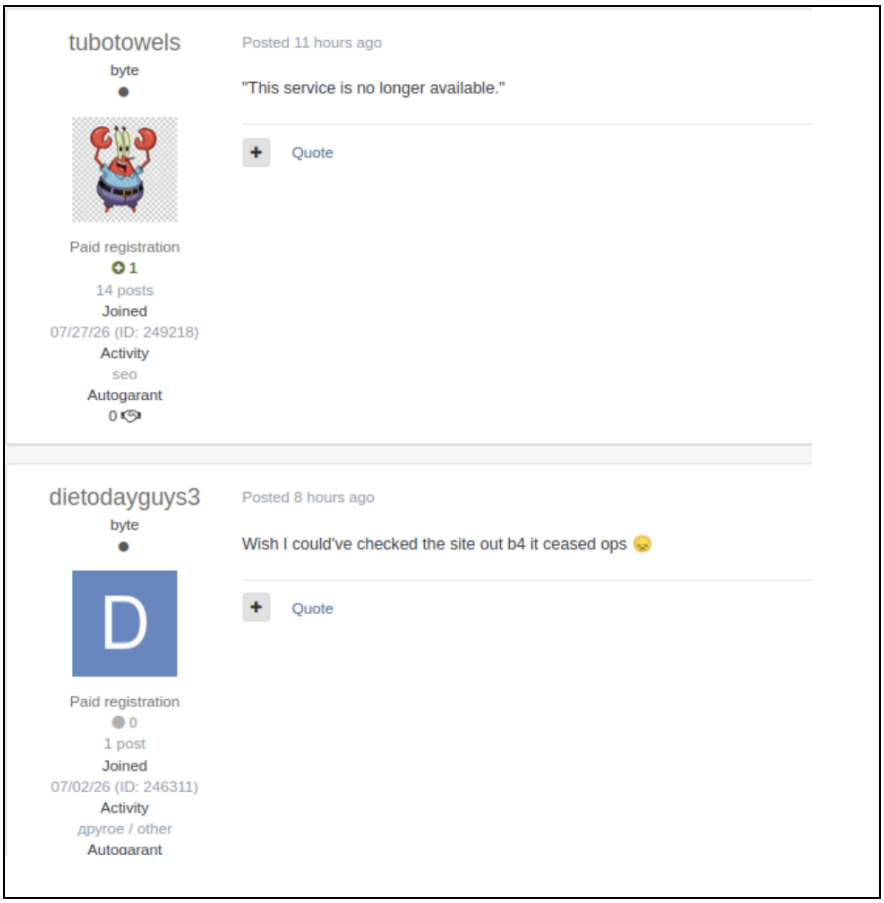
ZeroFox assesses that IDScan[.]net is very likely the vendor targeted by the threat actor; the company offers an identity verification platform in both digital and physical spaces. While IDScan[.]net has not made a public statement, several social media posts by customers claim that the company sent out an email about investigating a "potential security incident."

IDScan[.]net does not publicly list all of its clients, but some prominent known customers include:

- Shell
- Hertz
- General Motors
- Simmons Bank
- Caesars Entertainment
- Motorola
- Several other Fortune 500 companies[2]

While unconfirmed, it is almost certain that known government officials from both the United States and Canada were among those whose identity data was leaked. Further, the sheer size of the data set makes it almost certain that corporate executives, as well as customers of travel companies (including airlines and rental car companies), have been affected.

[2] hXXps://x[.]com/vxunderground/status/2095014197146861735



Two replies claiming the NEXUS portal has been shut down
Source: ZeroFox Intelligence

The threat actor, databroker1, is untested and recently registered on the Exploit forum. ZeroFox has observed some activity from a threat actor using the same handle on other dark web forums but cannot confirm their credibility at this time. However, if confirmed, this data breach would almost certainly be considered significant and would likely represent an ongoing threat for future exploitation.

As of September 2, 2026, the NEXUS portal has likely been shut down and is no longer accessible. This is not unusual, as threat actors commonly shut down or cash out quickly after major media attention focuses on a high-profile claim of a data breach or exposure. Additionally, no other threat actor has claimed access to the data outside of the NEXUS portal. However, there is a roughly even chance the data will spread beyond the portal and be used in future social engineering and phishing campaigns.

Although the portal is no longer active, there is a roughly even chance the threat actor will reactivate access after a cooling-off period to let the public scrutiny die down. Additionally, the threat actor's claim of persistence—as well as the extensive coverage of IDScan[.]net data potentially available—very likely makes this breach an ongoing threat to personal identity data.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%